Design and Development of Ransomware Response Framework using Selected Cybersecurity Models

A SYNOPSIS

Submitted for the Registration for the Degree

of

Doctor of Philosophy

in the

COMPUTER APPLICATION

Faculty of Science

by

Puneet Chauhan

Registration Number:
Enrolment Number: 2306000001497

Under the Supervision of

Dr. Shashiraj Teotia

Associate Professor & Head- Computer Application

Department of Computer Application

School of Science

Swami Vivekanand Subharti University

(NAAC Accredited grade "A" University)

Subhartipuram, NH-58, MEERUT-25005

(Year - 2023)

Table of Contents

1. INTRODUCTION 3

2. LITERATURE SURVEY 4

Rationale of the study ..... **Error! Bookmark not defined.**

3. RESEARCH GAP 6

4. RESEARCH OBJECTIVES 7

5. RESEARCH METHODOLOGY 8

Type of Research/ Design **8**

Population **8**

Sample/ Sampling Design **8**

Setting **8**

Method **8**

Intervention & duration **8**

Data Collection **9**

Assessment Tools **9**

Possible Prospective Outcomes **9**

6. REFERENCES 10

1. INTRODUCTION

In today's world the constant threat of cyber-attacks is a concern. Among these threats ransomware attacks stand out as challenging. Ransomware is a type of software that blocks access to a computer system or digital data until a payment is made. With the rise of "Ransomware as a Service" (RaaS) where attackers can access and use tools the potential for damage has increased significantly. To effectively counter these attacks, we need more than measures; we need a comprehensive strategy for response and recovery. This leads us to explore develop a comprehensive ransomware response framework as an area of research.

The reason behind adopting a strategic approach in crafting such a framework lies in the complexity and changing nature of cyber threats. Traditional security measures are no longer enough to combat the evolving strategies employed by cyber attackers. The availability of RaaS has made it easier for various actors to engage in campaigns leading to frequent and sophisticated attacks. Therefore, it is crucial that our response be equally sophisticated.

A scientific approach ensures that our strategy is methodical, and evidence based allowing us to continuously evaluate and adapt our response framework based on evolving threat landscapes. This approach also allows for the integration of various fields of knowledge through collating insights from computer science, cybersecurity, law, ethics, and geopolitical studies. The complexities of attacks go beyond the technical aspects; they involve legal, ethical, and geopolitical factors as well. By taking an approach we strive to gain an understanding and address these complex challenges effectively.

Given these difficulties our research aims to create a framework for responding to ransomware that is rooted in principles and best practices. Our goal is to equip organizations with the tools and knowledge to respond efficiently to attacks by facilitating swift recovery and minimizing harm. This involves developing robust incident response strategies and critically evaluating the associated legal, ethical, and geopolitical considerations.

Through adopting an approach in this research endeavour, we aspire to make contributions to the existing knowledge on cyber resilience. Our objective is to transform how organizations identify and address attacks by shifting their focus from measures, towards proactive resilience. Ultimately, we aim to create an environment where organizations are not only prepared for defending against ransomware attacks but also capable of recovering swiftly while maintaining the integrity of their operations and earning the trust of their stakeholders.

To summarize, the importance of taking a strategic and scientific approach to develop a framework for responding to ransomware lies in the necessity for a resilient and adaptable strategy that covers all aspects. This study aims to fulfil that need by creating a framework that remains strong amid changing cyber threats protecting resources and maintaining trust and integrity in the online realm.

2. LITERATURE SURVEY

Ransomware attacks have become increasingly prevalent and damaging in recent years, posing significant threats to individuals, corporations, and even nations **(Chidukwani et al., 2022)**. These attacks go beyond data breaches and privacy concerns, disrupting entire businesses, industries, supply chains, and critical infrastructure sectors. Many organizations have focused primarily on technology defences and prevention measures, neglecting other crucial aspects of cyber resilience building activities such as risk assessments, response planning, and training.

To address this issue, researchers, such as Baskerville et al. have proposed strategies to ensure a balanced approach to prevention and response in cybersecurity. In their study, the authors present a comprehensive taxonomy of ransomware and identify research directions in this area **(Zimba & Chishimba, 2019).**

Cascavilla et al. developed a detailed framework for devising effective ransomware response strategies. Their framework encompasses various components, including incident response plans, recovery procedures, and mitigation techniques. Additionally, the authors propose using the intelligence cycle as a systematic approach to study ransomware attacks and their implications **(Carrillo & García-Teodoro, 2022).**

However, while these studies provide valuable insights into ransomware attacks and response strategies, they do not thoroughly address the evolution of ransomware or classify attacks based on attack structures and underlying cryptosystems **(Zimba & Chishimba, 2019)**. In a study by Kok et al., the authors provided a short review of detection strategies and attack phases, highlighting the need for advanced and proactive response mechanisms.

Ethical, legal, and geopolitical concerns also play a crucial role in developing an effective ransomware response framework. Therefore, it is essential to consider the ethical, legal, and geopolitical considerations when building a comprehensive ransomware response framework. The study by **Sherer et al.** provides an overview of the ransomware's development and the general legal landscape, emphasizing the need for a multidimensional approach to address the complex nature of ransomware attacks.

Furthermore, organizations need to consider the potential ramifications of paying ransoms to cybercriminals.

This is where the study by **Pranshu Bajpai and Richard Enbody** becomes relevant, as they emphasize the need for a post-breach mindset that considers the ethical and legal implications of ransom payments. Additionally, the authors present a detailed ransomware response framework that addresses these concerns **(Bajpai & Enbody, 2023).** In their framework, **Bajpai and Enbody** emphasize the importance of proactive measures such as employee training, vulnerability assessments, and incident response planning.

Previous work in the field of ransomware response strategies has focused on various aspects, including prevention, detection, and mitigation techniques.

For instance, **Baskerville et al.** emphasized the importance of a balanced approach to prevention and response in cybersecurity. They proposed a strategy that includes risk assessments, response planning, and training to ensure cyber resilience.

Cascavilla et al. developed a detailed framework that encompasses incident response plans, recovery procedures, and mitigation techniques. They also suggested using the intelligence cycle as a systematic approach to study ransomware attacks and develop effective response strategies.

In terms of detection strategies, **Kok et al.** highlighted the need for advanced and proactive response mechanisms.

Maniath et al. addressed the challenges of ransomware attacks by proposing a hybrid approach that combines machine learning algorithms and behaviour-based analysis to detect and prevent ransomware infections.

Al-rimy et al. proposed a multi-layered defence system that includes network monitoring, antivirus software, and user awareness training to detect and mitigate ransomware attacks.

Furthermore, researchers have explored the use of honeypots and honey-files as decoys to attract and detect ransomware activity. **Fernández-Martínez et al (Bajpai & Enbody, 2023)** conducted a study on the effectiveness of honeypot-based ransomware detection and concluded that it can be an effective means of identifying and analysing ransomware attacks.

3. RESEARCH GAP

While extensive research has been conducted in the field of strategies to combat ransomware there are still areas that require attention.

1) One significant area, for exploration is the integration of principles into the development of frameworks to respond to ransomware incidents. Although previous studies have proposed solutions there is a need for more rigorous scientific evaluation and validation of these frameworks' effectiveness.
2) Another crucial aspect that needs to be addressed is the consideration of legal and geopolitical factors within ransomware response frameworks. This gap is significant because ransomware attacks have ranging consequences not for individuals and organizations but also for national security and global economic stability.

It is imperative to address concerns within response frameworks to ensure that any actions taken during and after an attack adhere to ethical standards and align, with legal and societal norms. Additionally considering factors becomes vital as ransomware attacks often transcend borders and may involve state sponsored actors or have political implications.

To bridge these research gaps, it is essential to develop a response framework that incorporates scientific principles while addressing ethical, legal, and geopolitical considerations.

4. RESEARCH OBJECTIVES

The main purpose of this study is to bridge the gaps in research that were mentioned earlier and offer a framework, for responding to ransomware incidents. This framework will be based on scientific principles and will also include ethical, legal, and geopolitical concerns. By incorporating scientific principles, the framework ensures that the proposed solutions are grounded in evidence-based practices and have undergone testing and validation.

This research aims at creating a flexible framework for responding to ransomware attacks, based on scientific principles and best practices. This involves studying how ransomware works, understanding the tactics used by attackers and developing a plan for addressing incidents. This research also aims to develop actionable guidelines for organizations in making decisions before, during, and after an attack.

Moreover, by addressing geopolitical concerns the framework provides guidelines and best practices for responding to ransomware attacks in line with international regulations while promoting lawful actions.

Furthermore, the framework recognizes the implications of attacks and offers strategies, for mitigating these risks. These strategies include fostering collaborations and facilitating information sharing.

The main objectives of this research are:

1) To study different types of ransomware attacks and to identify common patterns and unique characteristics.
2) To assess existing incident response protocols identifying their strengths and weaknesses.
3) To design and develop a ransomware response framework by incorporating legal, ethical, and geopolitical issues to counter global nature of cybercrime.

5. RESEARCH METHODOLOGY

Type of Research/ Design

This research adopts a mixed-methods design, integrating both qualitative and quantitative approaches to provide a comprehensive understanding of ransomware attacks and develop a robust response framework. The qualitative component involves expert interviews and case study analyses, while the quantitative aspect entails statistical analysis of past ransomware incidents.

Population

The study targets a broad population encompassing cybersecurity professionals, legal experts, policymakers, and organizations that have experienced ransomware attacks. This diverse population ensures a holistic perspective, capturing the technical, legal, ethical, and geopolitical dimensions of ransomware attacks.

Sample/ Sampling Design

A purposive sampling strategy will be employed to select participants who have direct experience with ransomware attacks or possess expert knowledge in cybersecurity. Approximately 10 cybersecurity professionals, 5 legal experts, 2 policymakers, and 2 organizations (representing a mix of those that have and have not experienced ransomware attacks) will be included in the sample.

Setting

The research will be conducted in a virtual setting, utilizing online platforms for interviews and surveys. This approach facilitates the participation of a diverse and geographically dispersed sample, ensuring a comprehensive understanding of ransomware attacks globally.

Method

To thoroughly examine attacks our research methodology includes conducting interviews, with experts analysing case studies and administering a survey. Through interviews and case study analyses we aim to gain an understanding of the intricate aspects of these attacks. Additionally, the survey will help us gather data regarding the frequency, consequences and countermeasures employed against attacks.

Intervention & duration

We aim to create a plan for dealing with attacks drawing on the information we've gathered from our research. The whole process is estimated to take a year during which we'll have time to collect data analyse it and develop the framework.

Data Collection
Data will be collected through semi-structured interviews with cybersecurity professionals, legal experts, and policymakers, as well as through surveys distributed to organizations. Additionally, case studies of past ransomware attacks will be analysed to extract patterns and insights.

Assessment Tools
The assessment tools will include an interview guide for the expert interviews, a structured survey questionnaire for organizations, and a case study analysis template. These tools are designed to ensure consistency in data collection and facilitate comprehensive analysis.

Possible Prospective Outcomes
The expected outcomes of this research include:

1) A scientifically grounded ransomware response framework, offering comprehensive strategies for prevention, mitigation, and recovery.
2) Enhanced understanding of the patterns and tactics used in ransomware attacks, aiding in predictive and preventive efforts.
3) Clear guidelines for organizations, incorporating technical, legal, ethical, and geopolitical considerations, to inform decision-making during ransomware incidents.
4) A contribution to the body of knowledge on cyber resilience, supporting future research and policy development in the field.

6. REFERENCES

Abely, C. (n.d.). *Ransomware, Cyber Sanctions, and the Problem of Timing*. *63*.

Aldauiji, F., Batarfi, O., & Bayousef, M. (2022). Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art. *IEEE Access*, *10*, 61695–61706. https://doi.org/10.1109/ACCESS.2022.3181278

Bajpai, P., & Enbody, R. (2023). Know Thy Ransomware Response: A Detailed Framework for Devising Effective Ransomware Response Strategies. *Digital Threats: Research and Practice*, *4*(4), 1–19. https://doi.org/10.1145/3606022

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges, and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

Cartwright, A., Cartwright, E., & Xue, L. (2019). Investing in Prevention or Paying for Recovery—Attitudes to Cyber Risk. In T. Alpcan, Y. Vorobeychik, J. S. Baras, & G. Dán (Eds.), *Decision and Game Theory for Security* (Vol. 11836, pp. 135–151). Springer International Publishing. https://doi.org/10.1007/978-3-030-32430-8_9

Cartwright, E., Hernandez Castro, J., & Cartwright, A. (2019). To pay or not: Game theoretic models of ransomware. *Journal of Cybersecurity*, *5*(1), tyz009. https://doi.org/10.1093/cybsec/tyz009

Connolly, L. Y., & Borrion, H. (2020). *Your Money or Your Business: Decision- Making Processes in Ransomware Attacks*.

Dey, D., & Lahiri, A. (2021). *Should We Outlaw Ransomware Payments?* Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2021.794

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: Views from a predictive model and human responses. *Crime Science*, *8*(1), 2. https://doi.org/10.1186/s40163-019-0097-9

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008

Kihiu, S., & Abade, E. (2020). *Comparative Analysis of Distinctive Features of the Ransomware Tactics in Relation to Other Malware*. *38*(1).

Porath, J. C. (n.d.). Typing a Terrorist Attack: Using Tools from the War on Terror to Fight the War on Ransomware. *PEPPERDINE LAW REVIEW*, *50*.

Ransomware Incident Preparations With Ethical Considerations and Command System Framework Proposal. (2022). *Journal of Leadership, Accountability and Ethics*, *19*(2). https://doi.org/10.33423/jlae.v19i2.5112

Robles-Carrillo, M., & Garcıa-Teodoro, P. (n.d.). Ransomware: An Interdisciplinary Technical and Legal Approach. *Security and Communication Networks*.

Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, Johor, 86400, Malaysia, Muslim, A. K., Mohd Dzulkifli, D. Z., Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, Johor, 86400, Malaysia, Nadhim, M. H., Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, Johor, 86400, Malaysia, Abdellah, R. H., & Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, Johor, 86400, Malaysia. (2019). A Study of Ransomware Attacks: Evolution and Prevention. *Journal of Social Transformation and Regional Development*, *1*(1). https://doi.org/10.30880/jstard.2019.01.01.003

Yuryna Connolly, A., & Borrion, H. (2022). Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. *Computers & Security*, *119*, 102760. https://doi.org/10.1016/j.cose.2022.102760

Yuryna Connolly, L., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1), tyaa023. https://doi.org/10.1093/cybsec/tyaa023